THE PROUHET-TARRY-ESCOTT PROBLEM FOR GAUSSIAN INTEGERS

TIMOTHY CALEY

ABSTRACT. Given natural numbers n and k, with $n > k$, the Prouhet-Tarry-Escott (PTE) problem asks for distinct subsets of $\mathbb{Z}$, say $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_n\}$, such that

$$x_1^i + \ldots + x_n^i = y_1^i + \ldots + y_n^i$$

for $i = 1, \ldots, k$. Many partial solutions to this problem were found in the late 19th century and early 20th century.

When $n = k - 1$, we call a solution $X =_{n-1} Y$ *ideal*. This is considered to be the most interesting case. Ideal solutions have been found using elementary methods, elliptic curves, and computational techniques. In 2007, Alpers and Tijdeman gave examples of solutions to the PTE problem over the Gaussian integers. This paper extends the framework of the problem to this setting. We prove generalizations of results from the literature, and use this information along with computational techniques to find ideal solutions to the PTE problem in the Gaussian integers.

1. INTRODUCTION

The Prouhet-Tarry-Escott problem, or PTE problem for short, is a classical number theoretic problem: given natural numbers n and k, with $k < n$, find two distinct subsets of $\mathbb{Z}$, say $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_n\}$, such that

$$\sum_{i=1}^{n} x_i^j = \sum_{i=1}^{n} y_i^j \quad \text{for } j = 1, 2, \ldots, k. \tag{1.1}$$

A solution is written $X =_k Y$, and n is its *size* and k is its *degree*. The maximal nontrivial case of the PTE problem occurs when $k = n - 1$. A solution in this case, say $X =_{n-1} Y$, is called *ideal*.

For example, $\{0, 3, 5, 11, 13, 16\} =_5 \{1, 1, 8, 8, 15, 15\}$ is an ideal PTE solution of size 6 and degree 5 since

$$\begin{aligned}
0 + 3 + 5 + 11 + 13 + 16 &= 48 = 1 + 1 + 8 + 8 + 15 + 15 \\
0^2 + 3^2 + 5^2 + 11^2 + 13^2 + 16^2 &= 580 = 1^2 + 1^2 + 8^2 + 8^2 + 15^2 + 15^2 \\
0^3 + 3^3 + 5^3 + 11^3 + 13^3 + 16^3 &= 7776 = 1^3 + 1^3 + 8^3 + 8^3 + 15^3 + 15^3 \\
0^4 + 3^4 + 5^4 + 11^4 + 13^4 + 16^4 &= 109444 = 1^4 + 1^4 + 8^4 + 8^4 + 15^4 + 15^4 \\
0^5 + 3^5 + 5^5 + 11^5 + 13^5 + 16^5 &= 1584288 = 1^5 + 1^5 + 8^5 + 8^5 + 15^5 + 15^5.
\end{aligned}$$

Date: February 15, 2011.

2000 *Mathematics Subject Classification.* Primary 11D72, 11Y50; Secondary 11P05.

The author would like to thank NSERC and the University of Waterloo for funding.

Similarly, for $a, b, c, d \in \mathbb{Z}$,

$$\{a+b+d, a+c+d, b+c+d, d\} =_2 \{a+d, b+d, c+d, a+b+c+d\},$$

is a family of PTE solutions of size 4 and degree 2 due to Goldbach. In fact, this example was also found by Euler for the case when $d = 0$. Many other elementary solutions can be found in [13].

The PTE problem is interesting because it is an old problem with both algebraic and analytic aspects, and also has connections to other problems. Ideal solutions are especially interesting because of their connection to problems in theoretical computer science [2] and combinatorics [16], a conjecture of Erdős and Szekeres [19, 12], [3, Chapter 13], as well as the "Easier" Waring problem, which we discuss below.

Given an integer k, the "Easier" Waring problem asks for the smallest n, denoted $v(k)$, such that for all integers m, there exist integers $x_1, \ldots, x_n$ such that

$$\pm x_1^k \pm \ldots \pm x_n^k = m,$$

for any choices of signs. This problem was posed by E. M. Wright as a weakening of the usual Waring's problem, which allows only addition. Note that $v(k)$ is conjectured to be $O(k)$. For arbitrary k, the best known bound is $v(k) \ll k \log(k)$ [3, Chapter 12], which is derived from the usual Waring's problem. For small values of k, the best bounds for $v(k)$ are derived from ideal solutions of the PTE problem. In fact, these are much better than those which derive from the usual Waring problem. See again [3, Chapter 12] for a full explanation of the connection between the two problems.

In 1935, Wright [26] conjectured that ideal solutions should exist for all n. However, it does not appear that this conjecture is close to being resolved. For $n = 2, 3, 4, 5$, complete parametric ideal solutions are known. For $n = 6, 7, 8$, only incomplete parametric solutions are known. See [3, Chapter 11] and [5, 8, 9] for further details of these cases. For $n = 10$, infinite inequivalent families of solutions are known (albeit incomplete) [23].

For size 9, only two inequivalent solutions are known. These were found computationally by P. Borwein, Lisoněk and Percival [4]. Until 2008, there were also only two inequivalent solutions known for size $n = 12$. They were both found computationally, by Kuosa, Myrignac and Shuwen [22] and Broadhurst [6]. However, in 2008, Choudhry and Wróblewski [11] found some infinite inequivalent families of solutions for $n = 12$ (again incomplete). Both infinite families of solutions for sizes 10 and 12 arise from rational points on elliptic curves using a method of Letac's from 1934, which appears in [15].

For $n = 11$ and $n \geq 13$, no ideal solutions are known.

Analytic methods are no closer to resolving Wright's conjecture. Along the same lines as the "Easier" Waring problem, define $N(k)$ to be the least n such that the PTE problem of degree k has a solution of size n. Much work has been done on obtaining upper bounds for $N(k)$, for example, see [17, 20, 26] and [3, Chapter 12]. The best upper bound is due to Melzak, which is $N(k) \leq \frac{1}{2}(k^2 - 3)$ when k is odd, and $N(k) \leq \frac{1}{2}(k^2 - 4)$ when k is even. Meanwhile, there is no lower bound on $N(k)$ that would rule out ideal solutions.

Although the PTE problem is traditionally looked at over $\mathbb{Z}$, it may be viewed over any ring. Alpers and Tijdeman [1] were the first to consider the PTE problem over a ring other than the integers. Their article discusses the PTE problem over

the ring $\mathbb{Z} \times \mathbb{Z}$ and shows that ideal solutions of size n in this case come from a particular kind of convex $2n$-gons. Their article also gives an example of a solution to the PTE problem over the Gaussian integers, $\mathbb{Z}[i]$. It further notes that there does not appear to be any other mention in the literature of the PTE problem in this setting. In [10], Choudhry examines the PTE problem over the ring of 2×2 integer matrices, $M_2(\mathbb{Z})$.

Based upon the work of Alpers and Tijdeman, because $\mathbb{Z}[i]$ contains $\mathbb{Z}$, we might expect smaller ideal solutions to the PTE problem in this setting. Therefore, this article examines ideal solutions to the PTE problem over $\mathbb{Z}[i]$. In particular, we view ideal solutions over $\mathbb{Z}$ as special cases of solutions over $\mathbb{Z}[i]$. We also describe a computational search for ideal solutions of size n for $\mathbb{Z}[i]$ for $n \geq 8$. This search generalizes the methods of Borwein, Lisoněk and Percival in [4]. They performed a computer search for ideal solutions of size $n = 10$ and $n = 12$, which took advantage of an alternative formulation of the problem to reduce the number of variables. Their search was further optimized by using the arithmetic properties of ideal solutions.

All the results that are required for the method of Borwein et al. generalize sufficiently to $\mathbb{Z}[i]$. We proceed by discussing some further background from the existing literature in Section 2, and then explaining the computational method to be used Section 3. In Section 4, we will provide analogues of existing theorems in the literature for the PTE problem over the Gaussian integers, which allow the computational search to be optimized. Finally in Section 6, we describe the results of a computational search for ideal solutions for $n = 10$ and $n = 12$.

For convenience, we state some results in greater generality than $\mathbb{Z}[i]$. As a general notation, we refer to the PTE problem over the ring R as the R-PTE problem. Throughout this article, let $\zeta \in \mathbb{C}$ be an algebraic integer, and let $\mathcal{O}$ denote the ring of integers of the number field $\mathbb{Q}(\zeta)$. Note that it is easy to find $\mathcal{O}$-PTE solutions, such as the example found by Goldbach given above. Hence, we proceed to discuss the PTE problem in this general setting.

2. Background

Solutions to the $\mathbb{Z}$-PTE problem satisfy many relations. Most of them generalize to $\mathcal{O}$ in a completely trivial way, and can easily be proved using Newton's identities. We list a few of them. Suppose $X = \{x_1, \ldots, x_n\}$ and $Y = \{y_1, \ldots, y_n\}$ are subsets of $\mathcal{O}$, and $k \in \mathbb{N}$ with $k \leq n - 1$. Then the following relations are equivalent:

$$\sum_{i=1}^{n} x_i^j = \sum_{i=1}^{n} y_i^j \quad \text{for } j = 1, 2, \ldots, k, \tag{2.1}$$

$$\deg\left(\prod_{i=1}^{n}(z - x_i) - \prod_{i=1}^{n}(z - y_i)\right) \leq n - k - 1, \tag{2.2}$$

$$(z-1)^{k+1} \Bigg| \sum_{i=1}^{n} z^{x_i} - \sum_{i=1}^{n} z^{y_i}. \tag{2.3}$$

Note that for any $c \in \mathbb{C}$, we have $z^c = e^{c \ln(z)}$. Since

$$\frac{d}{dz}(z^c) = \frac{d}{dz}\left(e^{c \ln(z)}\right) = c\frac{1}{z}e^{c \ln(z)} = cz^{c-1},$$

and we merely need differentiation for the proof of (2.2) $\iff$ (2.3), we can use this fact formally. Similarly, since the terms in the sum $\sum_{i=1}^n z^{x_i} - \sum_{i=1}^n z^{y_i}$ are not, in general, polynomials, we consider the division in (2.3) to refer to the order of the zero at 1. These relations provide an alternative formulation for the PTE problem.

Note that in particular, the relation (2.1) $\iff$ (2.2) implies that when $X =_{n-1} Y$,

$$\prod_{i=1}^n (z - x_i) - \prod_{i=1}^n (z - y_i)$$

is a constant in $\mathcal{O}$. This constant plays a significant role in the study of the PTE problem, which we discuss later in Sections 3 and 4.

Given a solution to the $\mathcal{O}$-PTE problem, we can generate an infinite family of solutions. That is, if $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_n\}$ are subsets of $\mathcal{O}$ with $\{x_1, \ldots, x_n\} =_k \{y_1, \ldots, y_n\}$, then

$$\{Mx_1 + K, \ldots, Mx_n + K\} =_k \{My_1 + K, \ldots, My_n + K\}, \tag{2.4}$$

for any $M, K \in \mathcal{O}$. This fact leads us to give the following definition:

Definition 2.1. Let $\mathbb{Q}(\zeta)$ be a number field and $\mathcal{O}$ be its ring of intgers. Suppose $X_1 =_k Y_1$ and $X_2 =_k Y_2$. If there exists an affine transformation $f(x) = Mx + K$ with M, K in $\mathbb{Q}(\zeta)$ such that $f(X_1) = X_2$ and $f(Y_1) = Y_2$, then we say that $X_1 =_k Y_1$ and $X_2 =_k Y_2$ are *equivalent*.

The following fact can be used as a criterion for PTE solutions to be equivalent. It will be useful later.

Proposition 2.2. *Suppose* $\{x_1, \ldots, x_n\} =_{n-1} \{y_1, \ldots, y_n\}$ *and* $\{x_1', \ldots, x_n'\} =_{n-1} \{y_1', \ldots, y_n'\}$ *are equivalent ideal* PTE *solutions via the transformation* $f(x) = Mx + K$ *where* $M, K \in \mathbb{Q}(\zeta)$. *If* $\prod_{i=1}^n (x - x_i) - \prod_{i=1}^n (x - y_i) = C$ *and* $\prod_{i=1}^n (x - x_i') - \prod_{i=1}^n (x - y_i') = C'$, *then* $C' = CM^n$.

Proof. If these solutions are equivalent, without loss generality, we may assume $Mx_i + K = x_i'$ and $My_i + K = y_i'$ for $i = 1, \ldots, n$. Thus, we have

$$\prod_{i=1}^n (x - (Mx_i + K)) - \prod_{i=1}^n (x - (My_i + K)) = C',$$

and since this holds for all values of x, we may replace x by $x + K$ to obtain

$$\prod_{i=1}^n ((x + K) - (Mx_i + K)) - \prod_{i=1}^n ((x + K) - (My_i + K)) = C'.$$

Simplifying, dividing through by M^n and then replacing x/M by x, we obtain

$$\prod_{i=1}^n (x - x_i) - \prod_{i=1}^n (x - y_i) = \frac{C'}{M^n},$$

proving the result. □

Let $\overline{z}$ denote the complex conjugate of z. It is clear that if $\{x_1, \ldots, x_n\} =_k \{y_1, \ldots, y_n\}$, then $\{\overline{x}_1, \ldots, \overline{x}_n\} =_k \{\overline{y}_1, \ldots, \overline{y}_n\}$ also.

3. Searching for Ideal Solutions Computationally

We might naively search for ideal solutions to the PTE problem over $\mathbb{Z}$ in the following way. Suppose our search space is $x_i, y_i \in [0, S] \cap \mathbb{Z}$. We may assume $x_1 = 0$. Then select the remaining integers so that $0 \leq x_2 \leq x_3 \leq \ldots \leq x_n$ and $1 \leq y_1 \leq \ldots \leq y_{n-1}$, and take $y_n = x_1 + \ldots + x_n - (y_1 + \ldots + y_{n-1})$. Now check whether or not

$$x_1^k + \ldots + x_n^k = y_1^k + \ldots + y_n^k$$

for each $k = 2, \ldots, n-1$. This method requires searching in $2n-1$ variables.

However, Borwein et al. [4] improve on this significantly. Recall from (2.2) that if $\{x_1, \ldots, x_n\} =_{n-1} \{y_1, \ldots, y_n\}$ is an ideal PTE solution, then

$$(z - x_1)(z - x_2)\cdots(z - x_n) - (z - y_1)(z - y_2)\cdots(z - y_n) = C,$$

for some constant $C \in \mathbb{Z}$. Rearranging this equation and then substituting $z = y_j$ for $j = 1, \ldots, n$ we obtain

$$(y_j - x_1)\cdots(y_j - x_n) = C. \tag{3.1}$$

For any $k \in \{1, \ldots, n\}$, equation (3.1) can be rearranged to

$$\frac{1}{C}(y_j - x_{n-k+2})\cdots(y_j - x_n) = \frac{1}{(y_j - x_1)\cdots(y_j - x_{n-k+1})}. \tag{3.2}$$

Now define

$$f(z) := \frac{1}{C}(z - x_{n-k+2})\cdots(z - x_n).$$

From (3.2), we have $f(y_j) = \frac{1}{(y_j - x_1)\cdots(y_j - x_{n-k+1})}$ for $j = 1, \ldots, k$. So if the variables $x_1, \ldots, x_{n-k+1}$ and $y_1, \ldots, y_k$ are known, then we also have the ordered pairs $(y_j, f(y_j))$ for $j = 1, \ldots, k$. We may determine $f(z)$ uniquely by using Lagrange polynomials and the ordered pairs $(y_j, f(y_j))$ for $j = 1, \ldots, k$ (see, for example [14, Chapter 5]). Thus, $f(x)$ is a polynomial of degree $k-1$, and solving $f(z) = 0$ yields its roots, which are $x_{n-k+2}, \ldots, x_n$. Repeating this process gives the remaining $y_{k+1}, \ldots, y_n$.

The method of Borwein et al. requires searching through only $n+1$ variables, instead of $2n-1$. This method can clearly be generalized to any ring of integers $\mathcal{O}$, and this is what we have implemented for $\mathcal{O} = \mathbb{Z}[i]$.

3.1. Optimizing the Search.

In order to explain how Borwein et al. further optimize the search over $\mathbb{Z}$, we need a definition, and in order to state it, we now restrict ourselves to any $\mathcal{O}$ that is also a unique factorization domain (UFD). We maintain this restriction for the remainder of this article.

Definition 3.1. Suppose $\mathcal{O}$ is a UFD. Suppose $X =_{n-1} Y$ is a $\mathcal{O}$-PTE solution with $\prod_{i=1}^{n}(z - x_i) - \prod_{i=1}^{n}(z - y_i) = C_{n,X,Y}$. Then let

$$C_n := \gcd\{C_{n,X,Y} | X =_{n-1} Y\}.$$

We say that C_n is the *constant associated* with the $\mathcal{O}$-PTE problem of size n.

Thus, C_n keeps track of all the common factors that appear among the constants that come from the second formulation of the PTE problem in (2.2). The requirement that $\mathcal{O}$ is a UFD is necessary for C_n to be well-defined.

We have the following Theorem, generalized from Proposition 3 in [4],

Theorem 3.2. *Suppose $\mathcal{O}$ is a* UFD. *Let $\{x_1, \ldots, x_n\} =_{n-1} \{y_1, \ldots, y_n\}$ be subsets of $\mathcal{O}$ that are an ideal $\mathcal{O}$-*PTE *solution. Suppose that $q \in \mathcal{O}$ is a prime such that $q \mid C_n$. Then we can reorder the y_i such that*

$$x_i \equiv y_i \pmod{q} \qquad \text{for } i = 1, \ldots, n.$$

The proof of Theorem 3.2 follows that of Proposition 3 from [4], but we repeat it for completeness.

Proof. Assume $q \in \mathcal{O}$ is a prime dividing C_n. Since $\mathcal{O}$ is an integral domain and q is prime, $\langle q \rangle$ is a prime ideal. Since prime ideals of rings of integers of number fields are also maximal (see, for example [24]), the quotient $\mathcal{O}/\langle q \rangle$ is a field. Let $\mathbb{F}_q$ denote this field. It follows that $\prod_{i=1}^{n}(z - x_i) - \prod_{i=1}^{n}(z - y_i)$ equals a constant times q, and so is zero in $\mathbb{F}_q[z]$. Hence, $\prod_{i=1}^{n}(z - x_i) = \prod_{i=1}^{n}(z - y_i)$ in $\mathbb{F}_q[z]$. Since $\mathbb{F}_q$ is a field, the polynomial ring $\mathbb{F}_q[z]$ is a unique factorization domain. Since each of the factors $z - x_i$ and $z - y_i$ are irreducible, it follows that the sets $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_n\}$ are equal as subsets of $\mathbb{F}_q$. That is, they are equal modulo q, as desired. □

Borwein et al. [4] use Theorem 3.2 to optimize the search for ideal solutions over $\mathbb{Z}$. This can also be applied over $\mathcal{O}$. Suppose q_1, q_2 are the two largest primes (in $\mathcal{O}$) dividing C_n. Assume $x_1 = 0$, and pick the rest of the variables so that for $i = 1, \ldots, n$

$$x_i \equiv y_i \pmod{q_1}$$
$$(x_{i+1} - y_i) \cdot \sum_{j=1}^{i}(x_j - y_j) \equiv 0 \pmod{q_2}.$$

We assume the solutions x_i and y_i pair modulo q_1, and that each x_i pairs to the previous y_i modulo q_2, unless all the x_j and y_j are already paired off modulo q_2. Hence, every prime q that divides C_n reduces the search space in each variable by a factor of $N(q)$, where $N(q)$ denotes the algebraic norm of q. Therefore, divisibility results, particularly large prime factors, for C_n are very important for optimizing the search.

4. Divisibility Results for C_n

There are a number of results in the literature concerning divisibility of C_n for the $\mathbb{Z}$-PTE problem. For example, about half of the article by Rees and Smyth [21] is spent proving such results. Many of these results generalize immediately to $\mathcal{O}$, which we state below without proof. In the case where the result is more of an analogy than a generalization, we provide a proof.

The usual method of generalization is to view arithmetic modulo a prime power in $\mathbb{Z}$ as analogous to arithmetic in the appropriate finite field, which is then viewed as analogous to arithmetic modulo the algebraic norm of a prime in $\mathcal{O}$. Fermat's Little Theorem corresponds with Lagrange's Theorem and so on. This method was used in the proof of Theorem 3.2 in the previous section.

The next two results are generalizations of Proposition 2.3 and Proposition 3.1 in [21], respectively.

Theorem 4.1. *Suppose $\mathcal{O}$ is a UFD. Let $q \in \mathcal{O}$ be a prime with $N(q) > 3$. Then $N(q) \mid C_{N(q)}$.*

Theorem 4.2. *Suppose $\mathcal{O}$ is a UFD. Let $q \in \mathcal{O}$ be a prime such that*

$$n + 3 \leq N(q) < n + 3 + \frac{n-2}{6}.$$

Then $q \mid C_{n+1}$.

Note that Rees and Smyth use a "Multiplicity Lemma" to prove this result in [21]. The proof of this lemma also generalizes appropriately to $\mathcal{O}$, and so Theorem 4.2 is remains valid.

We now prove a general divisibility result of C_n for powers of primes q. This result is based on the same techniques used in Proposition 2.4 of [21].

Proposition 4.3. *Suppose $\mathcal{O}$ is a UFD, and $q \in \mathcal{O}$ is a prime. If $q \mid C_n$, then*

$$q^{\lceil \frac{n}{N(q)} \rceil} \Big| C_n,$$

where $\lceil x \rceil$ denotes the smallest integer greater than x.

Proof. Suppose $X = \{a_1, \ldots, a_n\}$ and $Y = \{b_1, \ldots, b_n\}$ with $X =_{n-1} Y$, and $q \mid C_{n,X,Y}$. From Theorem 3.2, we can relabel the a_i and b_j such that $a_i \equiv b_i \pmod{q}$ for $i = 1, \ldots, n$. Note that $\mathcal{O}$ has $N(q)$ congruence classes modulo q, and so there is at least one congruence class with at least $\lceil n/N(q) \rceil$ elements from the set $\{b_1, \ldots, b_n\}$. Relabel this set so that $b_1, \ldots, b_{\lceil \frac{n}{N(q)} \rceil}$ are in the same congruence class modulo q. From equation (2.4), we can shift the a_i and b_i by $-b_1$, giving $C_{n,X,Y} = a_1 a_2 \cdots a_n$. Then

$$\begin{aligned} a_1 &\equiv b_1 \equiv 0 \pmod{q} \\ a_2 &\equiv b_2 \equiv 0 \pmod{q} \\ &\vdots \\ a_{\lceil \frac{n}{N(q)} \rceil} &\equiv b_{\lceil \frac{n}{N(q)} \rceil} \equiv 0 \pmod{q}. \end{aligned}$$

Thus, $q^{\lceil \frac{n}{N(q)} \rceil} \mid C_{n,X,Y}$, and since X and Y were arbitrary, we have proved the result. □

Note that we can only apply Proposition 4.3 when we already have from another source that $p \mid C_n$.

We now prove a specific result for the divisibility of C_5 for powers of primes $q \in \mathcal{O}$, with $N(q) = 2$. This result is based on the same techniques used in Proposition 2.5 of [21].

Proposition 4.4. *Suppose $q \in \mathcal{O}$ is prime with $N(q) = 2$. Then $q^4 \mid C_5$.*

Proof. Suppose $X = \{a_1, \ldots, a_5\}$ and $Y = \{b_1, \ldots, b_5\}$ with $X =_4 Y$. As in the proof of Proposition 4.3, we can relabel the a_i and b_j such that $a_i \equiv b_i \pmod{q}$ for $i = 1, \ldots, 5$, and so that $b_1, \ldots, b_3$ are in the same congruence class modulo q. Again as above, we can shift the a_i and b_i by $-b_1$, giving $C_{5,X,Y} = a_1 a_2 a_3 a_4 a_5$. Assume that $q^4 \nmid C_{5,X,Y}$. Since we know that $q^3 \mid C_{5,X,Y}$ however, we can assume that $a_1 \equiv a_2 \equiv a_3 \equiv q \pmod{q^2}$ and $a_4 \equiv a_5 \equiv 1 \pmod{q}$. As usual, we have

$$(z-a_1)(z-a_2)(z-a_3)(z-a_4)(z-a_5) - z(z-b_2)(z-b_3)(z-b_4)(z-b_5) = C_{5,X,Y}. \tag{4.1}$$

Substituting $z = a_1$ into (4.1) gives

$$-a_1(a_1 - b_2)(a_1 - b_3)(a_1 - b_4)(a_1 - b_5) = C_{5,X,Y}.$$

Since $a_1, a_1 - b_2, a_1 - b_3$ are all equivalent to 0 modulo q, while $a_1 - b_4, a_1 - b_5$ are both equivalent to 1 modulo q and their product is not divisible by q^4, we must have $a_1 \equiv a_1 - b_2 \equiv a_1 - b_3 \equiv q \pmod{q^2}$. Since $a_1 \equiv q \pmod{q^2}$ already, this means that $b_2 \equiv b_3 \equiv 0 \pmod{q^2}$.

We now substitute $z = a_4$ into (4.1) giving

$$-a_4(a_4 - b_2)(a_4 - b_3)(a_4 - b_4)(a_4 - b_5) = C_{5,X,Y}.$$

Since $a_4, a_4 - b_2, a_4 - b_3$ are all equivalent to 1 modulo q, while $a_4 - b_4, a_4 - b_5$ are both equivalent to 0 modulo q, we can assume, without loss of generality, that $a_4 - b_5 \equiv q \pmod{q^2}$ and $a_4 - b_4 \equiv q^2 \pmod{q^3}$, i.e., $a_4 - b_4 \equiv 0 \pmod{q^2}$.

Finally, substituting $x = b_5$ into (4.1) gives

$$(b_5 - a_1)(b_5 - a_2)(b_5 - a_3)(b_5 - a_4)(b_5 - a_5) = C_{5,X,Y}.$$

Only $b_5 - a_4$ and $b_5 - a_5$ are equivalent to 0 modulo q. However, we already have that $a_4 - b_5 \equiv q \pmod{q^2}$, and so we must have $a_5 - b_5 \equiv 0 \pmod{q^2}$. However, we have

$$\begin{aligned} 0 &= a_1 + a_2 + a_3 + a_4 + a_5 - (b_2 + b_3 + b_4 + b_5) \\ &\equiv q + q + q + b_4 + b_5 - 0 - 0 - b_4 - b_5 \equiv q \pmod{q^2}, \end{aligned}$$

which is a contradiction, proving the proposition. □

Not all results from the literature concerning C_n generalize to $\mathbb{Z}[i]$ or $\mathcal{O}$, and some must be addressed specifically depending on the ring of integers involved. Those relevant to our computer search for ideal solutions over $\mathbb{Z}[i]$ are discussed next.

5. Divisibility Results for C_n over $\mathbb{Z}[i]$

An important divisibility result for C_n over $\mathbb{Z}$ is that $n! \mid C_{n+1}$ (see Proposition 2.1 in [21], originally due to H. Kleiman in [18]). This fact demonstrates that C_n is highly composite and will contain some large prime factors. The proof that Rees and Smyth provide of Proposition 2.1 in [21] uses the obvious fact that if $t \in \mathbb{Z}$ then $t(t+1)(t+2)\dots(t+n) \equiv 0 \pmod{(n+1)!}$. However, this depends on t being an integer. Unfortunately, this fact does not fully generalize to $\mathbb{Z}[i]$. Nevertheless, we are able to state an analogous lemma below. For completeness, we prove this result in greater generality than necessary, that is, for the ring of integers of an arbitrary quadratic number field.

We first recall some facts concerning quadratic number fields from Chapter 5 of [7]. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with $d \neq 1$ squarefree and let $D = d(K)$ denote the discriminant of K, and let $\mathcal{O}$ be its ring of integers. We also assume that $\mathcal{O}$ is a UFD, but note that this hypothesis is not required for Propositions 5.1 and 5.2 or Lemma 5.3. We have the following results:

Proposition 5.1. (i) *If $d \equiv 1 \pmod 4$, then $\{1, \frac{1+\sqrt{d}}{2}\}$ is an integral basis for $\mathcal{O}$ and $D = d$.*

(ii) *If $d \equiv 2$ or $3 \pmod 4$, then $\{1, \sqrt{d}\}$ is an integral basis for $\mathcal{O}$ and $D = 4d$.*

Thus, we may write $\mathcal{O} = \mathbb{Z}[\omega]$, where $\omega = \frac{D+\sqrt{D}}{2}$.

Proposition 5.2. *Let p be a prime and $\left(\frac{a}{p}\right)$ be the Legendre symbol. Then the decomposition of prime ideals of $\mathbb{Z}$ in $\mathcal{O}$ is as follows:*

(i) *If $p \mid D$, i.e., if $\left(\frac{D}{p}\right) = 0$, then p is ramified, and we have $p\mathcal{O} = \mathfrak{p}^2$, where $\mathfrak{p} = p\mathcal{O} + \omega\mathcal{O}$, except when $p = 2$ and $D \equiv 12 \pmod{16}$. In this case $\mathfrak{p} = p\mathcal{O} + (1+\omega)\mathcal{O}$.*

(ii) *If $\left(\frac{D}{p}\right) = -1$, then p is inert, and hence $\mathfrak{p} = p\mathcal{O}$ is a prime ideal.*

(iii) *If $\left(\frac{D}{p}\right) = 1$, then p is split, and we have $p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_1 = p\mathcal{O} + \left(\omega - \frac{D+c}{2}\right)\mathcal{O}$ and $\mathfrak{p}_2 = p\mathcal{O} + \left(\omega - \frac{D-c}{2}\right)$, and c is any solution to the congruence $c^2 \equiv D \pmod{4p}$.*

Lemma 5.3. *Let $p \in \mathbb{Z}$ be a prime that is either ramified or split in $\mathcal{O}$, i.e., is of type (i) or (iii) from Proposition 5.2. Let $s \in \mathbb{N}$. Then*

$$t(t+1)(t+2)(t+3)\dots(t+sp-1) \in \begin{cases} \mathfrak{p}^s & \text{where } p \text{ is type (i) and } p\mathcal{O} = \mathfrak{p}^2, \\ \mathfrak{p}_1^s & \text{where } p \text{ is type (iii) and } p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2, \\ \mathfrak{p}_2^s & \text{where } p \text{ is type (iii) and } p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2. \end{cases}$$

Proof. Define a map $\phi : \mathcal{O} \to \mathbb{R}^2$ by $\phi(a + b\omega) = (a, b)$, where $a, b \in \mathbb{Z}$. Because $\{1, \omega\}$ is an integral basis for $\mathcal{O}$, it is clear that ϕ is well defined. We now examine the image of ramified and split ideals $p\mathcal{O}$ under ϕ.

First note that ω satisfies the equation $\omega^2 = \frac{D-D^2}{4} + D\omega$.

Suppose p is ramified. Then from Proposition 5.2, we have $p\mathcal{O} = \mathfrak{p}^2$, where $\mathfrak{p} = p\mathcal{O} + \omega\mathcal{O}$, excluding the case that $p = 2$ and $D \equiv 12 \pmod{16}$. Thus, an arbitrary element $q \in \mathfrak{p}$ looks like

$$\begin{aligned} q &= p(a + b\omega) + \omega(e + f\omega) \\ &= ap + (bp + e)\omega + f\omega^2 \\ &= ap + (bp + e)\omega + f\left(\frac{D - D^2}{4} + D\omega\right) \\ &= ap + f\left(\frac{D - D^2}{4}\right) + (bp + e + Df)\omega, \end{aligned}$$

where $a, b, e, f \in \mathbb{Z}$. Thus, we have

$$\phi(q) = \left(ap + f\left(\frac{D - D^2}{4}\right), bp + e + Df\right).$$

In the case that $p = 2$ and $D \equiv 12 \pmod{16}$, we have $\mathfrak{p} = p\mathcal{O} + (1+\omega)\mathcal{O}$. Thus, an arbitrary element $q \in \mathfrak{p}$ looks like

$$\begin{aligned} q &= p(a + b\omega) + (1 + \omega)(e + f\omega) \\ &= ap + e + (bp + e + f)\omega + f\omega^2 \\ &= ap + e + (bp + e + f)\omega + f\left(\frac{D - D^2}{4} + D\omega\right) \\ &= ap + e + f\left(\frac{D - D^2}{4}\right) + (bp + e + (D+1)f)\omega, \end{aligned}$$

where $a, b, e, f \in \mathbb{Z}$. Thus, we have

$$\phi(q) = \left(ap + e + f\left(\frac{D - D^2}{4}\right), bp + e + (D+1)f\right).$$

Alternatively, suppose p is split. Then from Proposition 5.2, we have $p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_1 = p\mathcal{O} + \left(\omega - \frac{d+c}{2}\right)\mathcal{O}$ and $\mathfrak{p}_2 = p\mathcal{O} + \left(\omega - \frac{D-c}{2}\right)$ and c is any solution to the congruence $c^2 \equiv D \pmod{4p}$.

Thus, an arbitrary element of $q \in \mathfrak{p}_1$ (resp. $\mathfrak{p}_2$) looks like

$$\begin{aligned} q &= p(a + b\omega) + \left(\omega - \frac{D \pm c}{2}\right)(e + f\omega) \\ &= ap + bp\omega + e\omega + f\omega^2 + f\left(\frac{D - D^2}{4} + D\omega\right) - \left(\frac{D \pm c}{2}\right)e + \left(\frac{D \pm c}{2}\right)f\omega \\ &= ap + f\left(\frac{D - D^2}{4}\right) - \left(\frac{D \pm c}{2}\right)e + \left(bp + e + fD + \left(\frac{D \pm c}{2}\right)f\right)\omega, \end{aligned}$$

where $a, b, e, f \in \mathbb{Z}$. Thus, we have

$$\phi(q) = \left(ap + f\left(\frac{D - D^2}{4}\right) - \left(\frac{D \pm c}{2}\right)e, \left(bp + e + fD + \left(\frac{D \pm c}{2}\right)f\right)\right).$$

Now let $t \in \mathcal{O}$ and suppose $t = u + v\omega$ so that $\phi(t) = (u, v)$. Note that $D \pm c$ is always even, and if we pick f so that $f\left(\frac{D-D^2}{4}\right)$ is an integer, then $\phi(q) \in \mathbb{Z}^2$ in all three of the above cases. Further, in each case, we may solve the equations $bp + e + Df = v$, $bp + e + (D+1)f = v$ and $bp + e + fD + \left(\frac{D\pm c}{2}\right)f = v$ for b, e, f. Thus, in each case, it follows that the set

$$\{t + jp, t + jp + 1, t + jp + 2, t + jp + 3, \ldots, t + jp + (p-1)\}$$

contains an element that belongs to $\mathfrak{p}$ or $\mathfrak{p}_1$ or $\mathfrak{p}_2$ respectively, for $j = 0, \ldots, s-1$. Thus, the set $\{t, t+1, t+2, \ldots, t+sp-1\}$ contains s elements that belong to $\mathfrak{p}$ or $\mathfrak{p}_1$ or $\mathfrak{p}_2$ respectively, proving the lemma. □

Remark 5.4. Note that if p is inert, i.e. of type (ii), the expression $t(t+1)(t+2)(t+3)\ldots(t+n)$ need not belong to $p\mathcal{O}$. For example, when $K = \mathbb{Q}(i)$ and $\mathcal{O} = \mathbb{Z}[i]$, $p = 3$ and $t = i$, note that none of $i, 1+i, 2+i, \ldots, n+i$ contain a factor of 3.

Using the above characterization of primes in a quadratic number field, we have the following result for the $\mathcal{O}$-PTE problem analogous to $n! \mid C_{n+1}$:

Theorem 5.5. *Let C_{n+1} be the constant associated with the $\mathcal{O}$-PTE problem. Suppose p is either (i) ramified or (iii) split and let*

$$\mathfrak{p} = \begin{cases} \mathfrak{p} & \text{where } p \text{ is type (i) and } p\mathcal{O} = \mathfrak{p}^2, \\ \mathfrak{p}_1 & \text{where } p \text{ is type (iii) and } p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2, \\ \mathfrak{p}_2 & \text{where } p \text{ is type (iii) and } p\mathcal{O} = \mathfrak{p}_1\mathfrak{p}_2 \end{cases}$$

Let $s = \lfloor (n+1)/p \rfloor$ and let ℓ be the highest power such that $n + 1 \in \mathfrak{p}^\ell$. Then $C_{n+1} \in \mathfrak{p}^{\max(s-\ell, 0)}$.

We digress before proving Theorem 5.5. As stated earlier, many results on the $\mathcal{O}$-PTE problem involve Newton's identities and symmetric polynomials, including the proof of (2.1) $\iff$ (2.2). We need them for the proof of some results below, so although they are well known and easily found in the literature (for example see [24]), we repeat them here.

Let $n \in \mathbb{N}$. Let $s_1, \ldots, s_n$ be variables. Then for all integers $k \geq 1$, we define

$$p_k(s_1, \ldots, s_n) := s_1^k + s_2^k + \ldots + s_n^k,$$

the kth power sum in n variables. Similarly, for $k \geq 0$, we define

$$\begin{aligned} e_0(s_1, \ldots, s_n) &= 1 \\ e_1(s_1, \ldots, s_n) &= s_1 + s_2 + \ldots + s_n \\ e_2(s_1, \ldots, s_n) &= \sum_{i<j} s_i s_j \\ &\vdots \\ e_n(s_1, \ldots, s_n) &= s_1 s_2 \cdots s_n \\ e_k(s_1, \ldots, s_n) &= 0, \forall k > n, \end{aligned}$$

to be the elementary symmetric polynomials in n variables. Then we have the result known as Newton's identities:

$$ke_k(s_1, \ldots, s_n) = \sum_{i=1}^{k} (-1)^{i-1} e_{k-i}(s_1, \ldots, s_n) p_i(s_1, \ldots, s_n), \tag{5.1}$$

for all $k \geq 1$. Note that this can be rearranged to

$$p_k(s_1, \ldots, s_n) = (-1)^{k-1} k e_k(s_1, \ldots, s_n) + \sum_{i=1}^{k-1} (-1)^{k-i} e_{k-i}(s_1, \ldots, s_n) p_i(s_1, \ldots, s_n), \tag{5.2}$$

for $k \geq 2$. Another fact is the identity

$$\prod_{i=1}^{n} (t - s_i) = \sum_{k=0}^{n} (-1)^k e_k(s_1, \ldots, s_n) t^{n-k}. \tag{5.3}$$

Thus, the coefficients of a polynomial are elementary symmetric polynomials of its roots, and because of (5.1), they depend on the power sums $p_i(s_1, \ldots, s_n)$.

We are now able to proceed with the proof of the Theorem.

Proof of Theorem 5.5. We closely emulate the proof of Proposition 2.1 in [21]. Suppose $X = \{x_1, \ldots, x_{n+1}\}$ and $Y = \{y_1, \ldots, y_{n+1}\}$ are subsets of $\mathcal{O}$, and $X =_n Y$. Then we have

$$(z - x_1) \cdots (z - x_{n+1}) - (z - y_1) \cdots (z - y_{n+1}) = C_{n+1,X,Y}$$

where $C_{n+1,X,Y} = (-1)^{n+1}(x_1 x_2 \cdots x_{n+1} - y_1 y_2 \cdots y_{n+1})$. Then from the identity (5.3), we have

$$\begin{aligned} (z - x_1) \cdots (z - x_{n+1}) &= \sum_{k=0}^{n+1} (-1)^k e_k(x_1, \ldots, x_{n+1}) z^{n+1-k} \\ (z - y_1) \cdots (z - y_{n+1}) &= \sum_{k=0}^{n+1} (-1)^k e_k(y_1, \ldots, y_{n+1}) z^{n+1-k}. \end{aligned}$$

From the identity (5.2), it follows that

$$\begin{aligned} p_{k+1}(x_1, \ldots, x_{n+1}) &= (-1)^k (k+1) e_{k+1}(x_1, \ldots, x_{n+1}) \\ &\quad + \sum_{i=1}^{k} (-1)^{k+1-i} e_{k+1-i}(x_1, \ldots, x_{n+1}) p_i(x_1, \ldots, x_{n+1}), \end{aligned} \tag{5.4}$$

and

$$p_{k+1}(y_1,\dots,y_{n+1}) = (-1)^k(k+1)e_{k+1}(y_1,\dots,y_{n+1}) + \sum_{i=1}^{k}(-1)^{k+1-i}e_{k+1-i}(y_1,\dots,y_{n+1})p_i(y_1,\dots,y_{n+1}). \tag{5.5}$$

By hypothesis, we have $p_k(x_1,\dots,x_{n+1}) = p_k(y_1,\dots,y_{n+1})$ and $e_k(x_1,\dots,x_{n+1}) = e_k(y_1,\dots,y_{n+1})$ for $1 \le k \le n$, and so subtracting (5.5) from (5.4) it follows that

$$\begin{aligned} p_{n+1}(x_1,\dots,x_{n+1}) - p_{n+1}(y_1,\dots,y_{n+1}) &= (-1)^n(n+1)e_{n+1}(x_1,\dots,x_{n+1}) \\ &\quad - (-1)^n(n+1)e_{n+1}(y_1,\dots,x_{y+1}). \end{aligned} \tag{5.6}$$

Now noting that $C_{n+1,X,Y} = e_{n+1}(x_1,\dots,x_{n+1}-e_{n+1})(y_1,\dots,y_{n+1})$, rearranging (5.6) we get

$$p_{n+1}(x_1,\dots,x_{n+1}) + (-1)^n(n+1)C_{n+1,X,Y} = p_{n+1}(y_1,\dots,y_{n+1}). \tag{5.7}$$

Since $s = \lfloor (n+1)/p \rfloor$, it follows that $sp < n+2$, and so from the above lemma we have

$$\sum_{k=0}^{n+1}(-1)^k e_k(0,-1,\dots,-n)t^{n+1-k} = t(t+1)(t+2)(t+3)\dots(t+n) \in \mathfrak{p}^s. \tag{5.8}$$

Substituting $t = x_1, x_2, \dots, x_{n+1}$ into (5.8) and summing, and doing the same for $t = y_1, y_2, \dots, y_{n+1}$, we get

$$\sum_{i=1}^{n+1}\sum_{k=0}^{n+1}(-1)^k e_k(0,-1,\dots,-n)x_i^{n+1-k} \in \mathfrak{p}^s \tag{5.9}$$

and

$$\sum_{i=1}^{n+1}\sum_{k=0}^{n+1}(-1)^k e_k(0,-1,\dots,-n)y_i^{n+1-k} \in \mathfrak{p}^s. \tag{5.10}$$

Subtracting (5.10) from (5.9) and applying (5.7), we get

$$(n+1)C_{n+1,X,Y} \in \mathfrak{p}^s.$$

Since $n+1 \in \mathfrak{p}^\ell$ and $n+1 \notin \mathfrak{p}^{\ell+1}$, we have $C_{n+1,X,Y} \in \mathfrak{p}^{\max(s-\ell,0)}$, and because X and Y were arbitrary solutions to the $\mathcal{O}$-PTE problem, we have $C_{n+1} \in \mathfrak{p}^{\max(s-\ell,0)}$, proving the theorem. □

The above divisibility results give lower bounds for C_n for the PTE problem over $\mathbb{Z}[i]$; these are stated in Table 1.

When $(*)$ appears in Table 1, this means the upper bounds for C_n come from the upper bounds for C_n for the PTE problem over $\mathbb{Z}$ (which we have included for comparison in Table 2). In the next section we explain the upper bounds new to the $\mathbb{Z}[i]$-PTE problem. These have been determined by searching for solutions computationally.

Table 2, which largely comes from [4, 5] but is updated with the new solutions from [6] and [11], shows that the constant for the $\mathbb{Z}$-PTE problem has many more factors than that for the $\mathbb{Z}[i]$- PTE problem. This demonstrates that the Gaussian

TABLE 1. Divisibility Results for the $\mathbb{Z}[i]$-PTE Problem

n	lower bound for C_n	upper bound for C_n
2	1	1
3	$(1+i)^2$	$(1+i)^2$
4	1	1
5	$(1+i)^4(2+i)(2-i)$	$(1+i)^5(2+i)(2-i)$
6	$(1+i)^3(2+i)(2-i)$	$(1+i)^4(2-i)^2(2+i)^2$
7	$(1+i)^4(2+i)(2-i)\cdot 3$	$(1+i)^6(2-i)^2(2+i)^2\cdot 3$
8	$(1+i)^4(2+i)(2-i)$	$(1+i)^8(2-i)^2(2+i)^2(3+2i)(3-2i)$
9	$(1+i)^5(2+i)(2-i)$ $\cdot 3^2\cdot(3+2i)(3-2i)$	$(1+i)^{18}(2-i)^2(2+i)^2\cdot 3^4\cdot 7^2\cdot 11\cdot(3+2i)$ $(-3+2i)(4+i)(4-i)\cdot 23\cdot(5+2i)(5-2i)$ $(*)$
10	$(1+i)^5(2+i)(2-i)$ $(3+2i)(3-2i)$	$(1+i)^{13}(2-i)^2(2+i)^2\cdot 3^2\cdot(3+2i)(-3+2i)$ $(4+i)(4-i)$
11	$(1+i)^6(2+i)^2(2-i)^2$	none known
12	$(1+i)^6(2+i)^2(2-i)^2$	$(1+i)^{24}(2-i)^3(2+i)^3\cdot 3^9\cdot 7^2\cdot 11^2\cdot(3+2i)^2$ $(-3+2i)^2(4+i)(4-i)\cdot 19\cdot 23\cdot(5+2i)$ $(5-2i)\cdot 31\,(*)$
13	$(1+i)^7(2+i)^2(2-i)^2$ $(3+2i)(3-2i)(4+i)(4-i)$	none known
14	$(1+i)^7(2+i)^2(2-i)^2$ $(3+2i)(3-2i)(4+i)(4-i)$	none known
15	$(1+i)^8(2+i)(2-i)$ $(3+2i)(3-2i)$	none known

TABLE 2. Divisibility Results for the $\mathbb{Z}$-PTE Problem

n	Lower bound for $C_n/(n-1)!$	Upper bound for $C_n/(n-1)!$
2	1	1
3	2	2
4	$2\cdot 3$	$2\cdot 3$
5	$2\cdot 3\cdot 5$	$2\cdot 3\cdot 5$
6	$2^2\cdot 3\cdot 5$	$2^3\cdot 3\cdot 5$
7	$3\cdot 5\cdot 7\cdot 11$	$2^2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 19$
8	$3\cdot 5\cdot 7\cdot 11$	$2^4\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13$
9	$3\cdot 5\cdot 7\cdot 11$	$2^2\cdot 3^2\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 23\cdot 29$
10	$5\cdot 7\cdot 13$	$2^4\cdot 3^2\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 23\cdot 37\cdot 53\cdot 61$ $\cdot 79\cdot 83\cdot 103\cdot 107\cdot 109\cdot 113\cdot 191$
11	$5\cdot 7\cdot 11\cdot 13\cdot 17$	none known
12	$5\cdot 7\cdot 11$	$2^4\cdot 3^5\cdot 5\cdot 7\cdot 11\cdot 13^2\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31$

integers are a much less restrictive setting for the PTE-problem than the ordinary integers.

6. Computer Search for Solutions

We may restrict the $\mathcal{O}$-PTE problem to a symmetric version. This is helpful because there are fewer variables, but at the same time, some ideal solutions may be missed. For odd n, this means finding solutions $x_1,\dots,x_n\in\mathcal{O}$ with $\{x_1,\dots,x_n\}=_{n-1}\{-x_1,\dots,-x_n\}$. Since $x_i^{2k}=(-x_i)^{2k}$ for all $k\in\mathbb{N}$, this means

we only need to consider solutions to $\sum_{i=1}^{n} x_i^e = 0$ for $e = 1, 3, \ldots, n-2$. For example, $\{3+3i, 3+4i, 3+5i, -2-8i, -7-4i\} =_4 \{-3-3i, -3-4i, -3-5i, 2+8i, 7+4i\}$ is an ideal symmetric solution of size 5.

Similarly, for even n, this means finding solutions $x_1, \ldots, x_{n/2}, y_1, \ldots, y_{n/2} \in \mathcal{O}$ such that $\{x_1, \ldots, x_{n/2}, -x_1, \ldots, -x_{n/2}\} =_{n-1} \{y_1, \ldots, y_{n/2}, -y_1, \ldots, -y_{n/2}\}$. As above, since $(-x_i)^{2e+1} = -x_i^{2e+1}$ for all $k \in \mathbb{N}$, we only need to consider solutions to $\sum_{i=1}^{n/2} x_i^e = \sum_{i=1}^{n/2} y_i^e$ for $e = 2, 4, \ldots, n-2$. For example, $\{\pm 1, \pm(4+i), \pm(3+i)\} =_5 \{\pm(7i), \pm(7+4i), \pm(7-3i)\}$ is an ideal symmetric solution of size 6.

Thus, the symmetric case of PTE problem involves half as many variables as the usual case. Some results concerning this case are discussed in [4, 8, 9].

In [4], Borwein et al. describe an algorithm for finding odd and even symmetric solutions to the $\mathbb{Z}$-PTE problem. We have adapted this algorithm for finding ordinary solutions as well as odd and even symmetric solutions to the $\mathbb{Z}[i]$-PTE problem. As the ideas behind the algorithms are not any different from the original, one may see [4] for an explanation. This was implemented first in *Maple* and then in `C++`, using the Class Library for Numbers.

The computer search was implemented to try to find solutions with real and imaginary parts between 0 and 30 for sizes 10 and 12. The above method is trivially parallelizable, so each search range was divided up into intervals, which were then submitted to a cluster of machines.

The following symmetric solutions of size 10 were found:

$$\{\pm(9+i), \pm(4+8i), \pm(8+4i), \pm(3-3i), \pm(1-9i)\} =_9$$
$$\{\pm(5+7i), \pm 8, \pm(9+3i), \pm 8i, \pm(1-7i)\}$$

which has constant

$$-(1+i)^{22}(2+i)^2(2-i)^2 3^2 (3+2i)^2 (3-2i)(4+i)(4-i)(5+2i),$$

and also

$$\{\pm(8+3i), \pm(9+4i), \pm(11+2i), \pm(1-7i), \pm(5+7i)\} =_9$$
$$\{\pm(7+7i), \pm(11+1i), \pm(11+4i), \pm(1+6i), \pm 5i\}$$

which has constant

$$i(1+i)^{13}(2+i)^2(2-i)^2 3^2 (3+2i)^2 (3-2i)(4+i)(4-i)(5+2i)(5-2i)(5+4i).$$

Additionally, by the remark at the end of Section 2, the complex conjugates of these solutions are also ideal PTE solutions of size 10. First note that none of these solutions lies on a line in the complex plane. Thus they cannot be equivalent to a $\mathbb{Z}$-PTE solution. By examining their constants and applying Proposition 2.2, they cannot be equivalent to each other either.

Further note that all the Gaussian integers in the first solution have norm ≤ 90, while in the second they all have norm ≤ 147. This contrasts with the ordinary integer case where from [4] there is no size 10 solution with height less than 313, and in fact, there are only two inequivalent solutions with height less than 1500. This results corresponds to the intuition that Gaussian integer solutions should be "easier" to find.

We now explain the second column of Table 1 above, which lists the upper bounds for the divisibility of C_n.

For $n = 2$ and $n = 3$, the upper bound comes from Table 2.

For $n = 4$, the upper bound comes from the solution $\{0, 0, 0, 0\} =_3 \{1, -1, i, -i\}$.

For $n = 5$, the solutions

$$\{0, -5i, -3 - 4i, 1 + 3i, 1 + 3i\} =_4 \{-5 - 5i, 5, -4 + 3i, 1 - 7i, 2 + 6i\}$$

and

$$\{0, 2 - 4i, 3 - i, -6 - 3i, -4 - 7i\} =_4 \{-5 - 5i, -4 - 2i, 4 - 3i, -2 - 6i, 2 + i\}$$

have constants $-(1+i)^5(2-i)^2(2+i)^7$ and $i(1+i)^6(2-i)(2+i)^6$ respectively. The upper bound comes from taking the gcd of these constants, along with the constant associated to the complex conjugate of the second solution.

For $n = 6$, the solution

$$\{0, -5i, 2-4i, -4-2i, -6+2i, -4+3i, -5-5i\} =_5 \{-5+5i, 1+3i, -8+i, 1-7i, 4-3i\}$$

has constant $-(1+i)^4(2-i)^2(2+i)^8(-3+2i)$. The upper bound comes from taking the gcd of this constant and the constant associated to the complex conjugate of this solution.

For $n = 7$, the solution

$$\{3 + i, 2 + 4i, -3 - 4i, 2 - 3i, -5 + 2i, -5 + 3i, 6 - 3i\} =_6 \{-3 - i, -2 - 4i, 3 + 4i, -2 + 3i, 5 - 2i, 5 - 3i, -6 + 3i\},$$

has constant $(-i)(1 + i)^6(2 - i)^3(2 + i)^2 3(3 + 2i)(4 + i)(5 - 2i)$. The upper bound comes from taking the gcd of this constant and the constant associated to the complex conjugate of this solution.

For $n = 8$, the symmetric solution

$$\{\pm(2 + 2i), \pm 3, \pm 3i, \pm(2 - 2i)\} =_7 \{\pm 2, \pm 2i, \pm i, \pm 1\}$$

has constant $(1 + i)^8(2 - i)^2(2 + i)^2(3 + 2i)(-3 + 2i)$.

For $n = 10$, the upper bound is obtained taking the gcd of the constants from the solutions listed above, as well as their complex conjugates.

For $n = 9$ and $n = 12$, the upper bound is obtained from factoring the bounds listed in Table 2.

Note that for n in the range $4 \leq n \leq 8$, many other $\mathbb{Z}[i]$-PTE solutions are known, but they give no further information about the divisibility of C_n. In these cases, we have not been able to prove if these upperbounds are true in general.

Unfortunately, no symmetric solutions of size 12 have been found. Considering that there is a symmetric solution of size 12 of height 151 in the integer case, the usual intuition implies that a Gaussian integer solution would not be much larger than the search range. However, the search for size 12 ideal solutions took approximately 2 weeks on a cluster of 16 machines each with four 1Ghz. processors. Considering the magnitude of the solutions found in the integer case, this method does not seem likely to produce them in the Gaussian integer case.

7. Further Work

There are some natural directions for further work in this area. Clearly, the search range could be extended with the aim of finding more ideal solutions over the Gaussian integers. Additionally, since Theorem 5.5 (as well as the results in Section 4) holds for any ring of integers of a quadratic number field that is a unique factorization domain, a computer search as described in the previous section is certainly possible in any such ring.

However, our current implementation does not readily generalize to any ring of integers. Further, we believe that any implementation of a computer search in a different ring of integers would be significantly computationally slower than that for $\mathbb{Z}[i]$. This is because for most mathematical software, determining whether or not a complex number is a Gaussian integer is naturally much easier than determining whether or not it is, say, an element of $\mathbb{Z}[e^{2\pi i}]$.

We are currently working on another computational method which would generalize the work of Smyth in [23] and Choudhry and Wróblewski in [11]. Both of these articles relate the $\mathbb{Z}$-PTE problem to elliptic curves.

8. Acknowledgements

I would like to thank my supervisor Kevin G. Hare for his support and advice. I would also like to thank the referee for his careful reading of the paper and many helpful comments.

References

1. A. Alpers and R. Tijdeman, *The two-dimensional Prouhet-Tarry-Escott problem*, J. Number Theory **123** (2007), 402–412.
2. B. Borchert, P. McKenzie, and K. Reinhardt, *Few Product Gates But Many Zeros*, Lecture Notes in Computer Science No. 5734, 162–174.
3. P. Borwein, *Computational Excursions in Analysis and Number Theory*, CMS books in mathematics 10, Springer-Verlag, New York, 2002.
4. P. Borwein, P. Lisoněk and C. Percival, *Computational investigations of the Prouhet-Tarry-Escott problem,* Math. Comp. **72** (2003), 2063–2070.
5. P. Borwein, C. Ingalls, *The Prouhey-Tarry-Escott Problem revisited,* Enseign. Math. **40** (1994), 3–27.
6. D. Broadhurst, A Chinese Prouhet-Tarry-Escott solution `http://physics.open.ac.uk/~dbroadhu/cpte.pdf`, 2007.
7. H. Cohen, *A Course in Computational Algebraic Number Theory.* Springer-Verlag, Berlin, 1993.
8. A. Choudhry, *Ideal solutions of the Tarry-Escott problem of degree four a related Diophantine system*, Enseign. Math. (2) **46** (2000), no. 3-4, 313–323.
9. A. Choudhry, *Ideal solutions of the Tarry-Escott problem of degrees four and five and related Diophantine systems*, Enseign. Math. (2) **49** (2003), no. 1-2, 101–108.
10. A. Choudhry, *Matrix analogues of the tarry-Escott problem, multigrade chains and the equation of Fermat*, Math. Student **75** (2006), no. 1-4, 215–224.
11. A. Choudhry, J. Wróblewski, *Ideal Solutions of the Tarry-Escott Problem of degree eleven with applications to Sums of Thirteenth Powers,* Hardy-Ramanujan J. **31** (2008), 1–13.
12. M. Cipu, *Upper bounds for norms of products of binomials*, LMS J. Comput. Math. **7** (2004), 37–49.
13. L. E. Dickson, *History of the Theory of Numbers Vol. II*, Chelsea Publ. Co., New York, 1971.
14. J. von zur Gathen and J. Gerhard, *Modern Computer Algebra, 2nd edition.* Cambridge University Press, London, 2003.
15. A. Gloden, *Mehrgradige Gleichungen*, Noordhoff, Groningen, 1944.
16. S. Hernández and F. Luca, *Integer Roots Chromatic Polynomials of Non-Chordal Graphs and the Prouhet-Tarry-Escott Problem*, Graphs and Combinatorics **21** (2005), 319–323.
17. L. K. Hua, *Introduction to Number Theory*, Springer-Verlag, New York, 1982.
18. H. Kleiman, *A note on the Tarry-Escott problem*, J. Reine Angew. Math. **278/279** (1975), 48–51
19. R. Maltby, *Pure product polynomials and the Prouhet-Tarry-Escott problem*, Math. Comp. **66** (1997), 1323–1340
20. Z. A. Melzak, *A note on the Tarry-Escott problem*, Canad. Math. Bull. **4** (1961), 233–237.
21. E. Rees and C. Smyth, *On the Constant in the Tarry-Escott Problem*, Lecture Notes in Mathematics 1415, Springer, Berlin, 1990, 196–208.

22. C. Shuwen, The Prouhet-Tarry-Escott Problem. `http://euler.free.fr/eslp/TarryPrb.htm`
23. C. J. Smyth, *Ideal 9th-Order Multigrades and Letac's Elliptic Curve*, Math. Comp., **57**, (1991), 817-823.
24. I. Stewart, D. Tall, *Algebraic Number Theory and Fermat's Last Theorem,* AK Peters, Massachusetts, 2002.
25. E. M. Wright, *An easier Waring's problem*, J. London Math. Soc., **9** (1934), 267–272.
26. E. M. Wright, *On Tarry's problem (I)*, Quart. J. Math., Oxford Ser. **6** (1935), 261–267.
27. E. M. Wright, *Prouhet's 1851 solution of the Tarry-Escott problem*, Amer. Math. Monthly **66** (1959) 199–201.

Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1

E-mail address: `tcaley@math.uwaterloo.ca`